

Rocket Fibre

Privacy Policy

Version 2.0 | Effective from 1 September 2026 | www.rocket-fibre.co.uk

1. About this policy

1.1 Rocket Fibre Ltd (registered number 12821973) is the controller of the personal data described in this policy. Our registered office is Unit 5 Perth House, Corby Gate Business Park, Corby, Northamptonshire, NN17 5JG. In this policy “we”, “us” and “our” mean Rocket Fibre Ltd, trading as Rocket Fibre, and “you” means the person whose personal data we hold.

1.2 This policy explains what personal data we collect, why we collect it, who we share it with, how long we keep it and the rights you have. It applies to our residential and business broadband and telephone services; our mobile services; our wholesale, carrier and interconnection services, including services carried over our network (AS8801); our colocation and data centre services; our website at rocket-fibre.co.uk, our customer portal and our social media pages; and to anyone who contacts us, visits our premises or deals with us on behalf of a customer, supplier or partner.

1.3 Rocket VPN is covered by the separate VPN Privacy Policy on our website. Job applicants and members of our staff are covered by separate privacy notices that we provide when you apply or join. Cookies and similar technologies are explained in more detail in our Cookie Policy.

1.4 We are required to comply with the UK General Data Protection Regulation and the Data Protection Act 2018, each as amended by the Data (Use and Access) Act 2025; the Privacy and Electronic Communications (EC Directive) Regulations 2003; and the Communications Act 2003 and the General Conditions of Entitlement set by Ofcom. In this policy we call these laws, together, “data protection law”.

1.5 In summary: we use your personal data to check what we can provide at your address, to set up, run, secure and bill the services you order, to support you, to meet our legal duties as a communications provider and, with your permission or where the law allows, to tell you about our services. We do not sell personal data.

2. How to contact us about your personal data

2.1 Our data protection team is responsible for this policy and for handling your requests, questions and complaints. You can reach them by email at hello@rocket-fibre.co.uk; by telephone on 0330 1227 711 (Monday to Friday 9am to 5pm, Saturday 9am to 4pm); through the contact form on our website; or by post to Data Protection, Rocket Fibre Ltd, Unit 5 Perth House, Corby Gate Business Park, Corby, Northamptonshire, NN17 5JG.

2.2 Please mark postal correspondence and email subject lines “Data Protection” so that we can direct it to the right team without delay.

3. The personal data we collect

3.1 Information you give us

3.1.1 When you enquire, order, register for the portal or contact us, we collect: your name, address, email address and telephone numbers; your date of birth where we need

it for identity or credit checks; the address at which services are to be provided and any access instructions; your account, order and package details, including your portal login details and security answers; your payment details, which for residential services means the card details our payment provider needs to take payment (we do not store full card numbers ourselves) and, for business and wholesale customers, bank account details for Direct Debit or invoice payment; copies of identity documents where we verify who you are; what you tell us in calls, emails, web chat, letters, complaints and surveys; and your marketing preferences.

3.1.2 If you tell us about a disability, a health condition or other circumstances that mean you need additional support, or that someone at your premises relies on a telecare, health or security device connected to the line, we record that information so that we can support you properly and meet our obligations to Ofcom (see clause 4.6). This can include information about your health, which is a special category of personal data under data protection law.

3.1.3 If you give us information about other people, such as members of your household, an authorised contact, a nominated person to manage your account or the people you want to admit to our data centre, you must make sure they are happy for you to do so and have seen this policy.

3.2 Information we collect when you use our services

3.2.1 To provide connectivity we generate and hold technical data, including the IP addresses we allocate to you, the identifiers (such as MAC addresses and serial numbers) of the router, optical network terminal and other equipment on your connection, line status, sync speed and performance measurements, and the results of speed tests.

3.2.2 We hold traffic and usage data about your services, including the volume, timing and duration of sessions and connections and, for telephone services, the numbers you call and are called from, the calling line identity presented, and the time and length of each call. We do not read, listen to or store the content of your communications, other than voicemail, email and messaging services that you ask us to provide and the call recordings described in clause 4.9.

3.2.3 For mobile services we also hold the SIM, IMSI and IMEI identifiers of your SIM and handset, the cell and location data generated by the mobile network when you use your device, and roaming and usage records supplied by the mobile network operator.

3.2.4 When you use our website or portal we collect your IP address, device and browser details, the pages you visit and the actions you take, together with the cookie and similar data described in our Cookie Policy. We keep records of your portal logins for security.

3.2.5 We keep records of every installation, engineer visit, fault, service change and contact with you, and of switching and number porting requests made through the industry switching hub or another provider.

3.3 Information we receive from other people. We receive personal data from: credit reference agencies and fraud prevention agencies (see section 7); the network operator whose infrastructure serves your premises (the "Infrastructure Provider" named in your Order), including availability, appointment, installation and fault information; the mobile network operator that carries our mobile services; other communications providers and the switching hub operated by The One Touch Switching Company (TOTSCo) when you switch to or from us or port a number; resellers, partners and wholesale customers who order services on your behalf; our payment providers; publicly available sources such as Companies House and the RIPE Database; social media platforms when you interact with our pages; and public authorities, regulators and dispute resolution bodies in the course of their functions.

3.4 Visitors to our data centres and offices. If you visit our data centre or offices we collect your name, employer, the details of the identity document you present, your vehicle registration if you park on site, your entry and exit times and the access cards, codes or areas you use, and CCTV images. Where a colocation customer adds you to its Access List we hold the details the customer gives us for that purpose.

3.5 Business, wholesale and partner contacts. If you deal with us on behalf of a business customer, wholesale or carrier customer, supplier or partner, we hold your name, job title, employer, work contact details and the records of our dealings with you, including contract, order, ticket, letter of authority and cross-connect records. Technical and abuse contact details for networks we peer or interconnect with are recorded in the RIPE Database and PeeringDB in accordance with the rules of those registries.

4. How we use your personal data and the legal grounds we rely on

Data protection law only allows us to use personal data if we have a lawful basis for doing so. The purposes we use your personal data for, and the basis we rely on for each, are set out below. Where more than one basis applies we have listed each of them.

4.1 Checking availability and setting up your service. We use the address and contact details you give us to check what we and our Infrastructure Providers can deliver at your premises, to give you a quote and Contract Summary, and to place and manage your order and installation. Basis: taking steps at your request before entering a contract, and performing our contract with you.

4.2 Providing and managing your services. We use your account, technical, traffic and usage data to connect, activate, deliver, support and change your services, to send you service messages, and to keep records of what we have provided. Basis: performing our contract with you, and complying with our legal obligations under the Communications Act 2003 and Ofcom's General Conditions.

4.3 Running and securing our network. We monitor traffic, connections and equipment on our network to keep it working, to plan capacity, to apply our Traffic Management Policy, and to detect and stop attacks, malware, spam, abuse and fraud. Basis: our legitimate interest in the security of our network and information systems, which data protection law recognises as a legitimate interest, and our legal obligations under the Telecommunications (Security) Act 2021 and the Electronic Communications (Security Measures) Regulations 2022.

4.4 Billing and payment. We use your account, usage and payment details to calculate and send bills, to take payment, to manage credits, refunds and deposits, and to recover money you owe, including through debt collection agencies and the

courts. Basis: performing our contract with you, and our legitimate interest in being paid for the services we provide.

4.5 Credit, identity and fraud checks. Before we provide services, and from time to time while you are a customer, we check your identity and creditworthiness and screen for fraud, using the agencies described in section 7. Basis: our legitimate interest in managing credit risk and preventing fraud, the recognised legitimate interest in the prevention and detection of crime, and, where a check is required by law, our legal obligations.

4.6 Supporting customers who need additional help. We record the support needs you tell us about so that we can offer priority fault repair, accessible formats, a nominated third party for your account and other help, and so that we can meet our obligations to Ofcom to treat vulnerable customers fairly and to protect people who rely on telecare and similar devices, including during the migration from traditional landlines. Basis: our legal obligations under Ofcom's General Conditions and, for information about your health, your explicit consent or, where the law requires us to hold it, the substantial public interest conditions in Schedule 1 to the Data Protection Act 2018. You can ask us to update or remove this information at any time.

4.7 Switching and number porting. When you join or leave us we exchange the information needed to switch your service, port your number and stop you paying twice, through the industry switching hub and with your other provider. Basis: our legal obligations under Ofcom's General Conditions on switching and number portability, and performing our contract with you.

4.8 Customer service, complaints and disputes. We use your records to answer enquiries, resolve faults, handle complaints under our Complaints Code of Practice, and deal with disputes, including through the Communications Ombudsman and the courts. Basis: performing our contract with you, our legal obligations, and our legitimate interest in resolving issues and defending our position.

4.9 Recording and monitoring calls and messages. We may record and monitor telephone calls, web chats and emails with you for training, quality, security and fraud prevention purposes and to keep evidence of instructions and agreements. Basis: our legitimate interests in those purposes, in accordance with the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000. We tell you at the start of a call if it is being recorded.

4.10 Marketing. We may tell you about our services, offers and news by email, text, telephone, post and through our portal. If you are an existing customer, or you have enquired about our services, we may contact you about similar services of ours by email or text unless you have told us not to. In all other cases we will only send electronic marketing with your consent. You can opt out at any time using the link in any message, by replying STOP to a text, or by contacting us. Basis: our legitimate interest in promoting our business, which data protection law recognises as a legitimate interest, and your consent where the Privacy and Electronic Communications Regulations require it.

4.11 Improving our services. We analyse how our services, website and portal are used, and the outcome of orders, faults and complaints, so that we can improve them and plan our network. Wherever practicable we do this using aggregated or anonymised information that does not identify you. Basis: our legitimate interest in improving what we offer.

4.12 Meeting our legal duties as a communications provider. We hold, and where required disclose, communications data and other records to meet our obligations under the Investigatory Powers Act 2016, the

Communications Act 2003 and the Online Safety Act 2023, and to respond to lawful requests and orders from Ofcom, the emergency services, the police and other public authorities and the courts. Section 5 explains this in more detail. Basis: our legal obligations, and the recognised legitimate interests in responding to requests from public authorities, in preventing and detecting crime, in safeguarding vulnerable people and in responding to emergencies.

4.13 Protecting our premises, people and equipment. We operate CCTV, access control and visitor registration at our data centres and offices, verify the identity of visitors and keep records of who has accessed which areas and when. Basis: our legitimate interest in the security of our sites and of the equipment our customers entrust to us, and performing our contracts with colocation customers.

4.14 Managing business relationships. We use the details of the people we deal with at business customers, wholesale and carrier customers, suppliers and partners to negotiate and perform contracts, manage orders, tickets, interconnections and peering, and keep in touch. Basis: performing our contracts and our legitimate interest in running our business.

4.15 Corporate transactions. If we buy or sell a business, raise finance or reorganise, we may share personal data with the other parties and their advisers, and any successor may use it in the way described in this policy. Basis: our legitimate interest in developing our business.

4.16 Where we rely on legitimate interests we have considered whether our interests are outweighed by the impact on you, and we have concluded that they are not. You have the right to object to any processing based on legitimate interests (see section 12). Data protection law also lists certain “recognised legitimate interests”, such as responding to requests from public authorities and preventing crime, for which that balancing exercise is not required. Where we rely on a recognised legitimate interest we still only use the personal data that is necessary for the purpose.

4.17 We will only use your personal data for a purpose that is not covered by this policy if that purpose is compatible with the original one, or if data protection law otherwise allows or requires it. If we need your consent for a new purpose we will ask for it first.

5. Communications data, lawful requests and the law

5.1 We provide public electronic communications networks and services, which brings specific legal duties. We may be required by notice under the Investigatory Powers Act 2016 to retain communications data, such as records of the calls made and the connections established over our services, for up to twelve months, and to disclose communications data and provide other assistance to the police, the security and intelligence agencies and other public authorities where they have lawful authorisation to obtain it. In most cases the law prevents us from telling you about these notices and requests.

5.2 We provide the information needed to route 999 and 112 calls and to give the emergency services the name, address and calling number associated with your telephone service, through the emergency services database. If you take a telephone service and ask to be listed, we pass your name, address and number to directory and directory enquiry providers; you can ask to be ex-directory at any time.

5.3 We may be required to block access to particular websites or services by court order, including orders made under the Copyright, Designs and Patents Act 1988 and the Online Safety Act 2023, and to comply with information requests from Ofcom under the Communications Act 2003.

5.4 Apart from the cases described in this section and in clause 4.3, we do not monitor, intercept or disclose the content of your communications or your communications data unless the law requires or permits us to do so.

6. Who we share your personal data with

We share personal data only where it is necessary for the purposes described in section 4, and only the data that each recipient needs. We share it with:

6.1 Infrastructure Providers. The network operator whose fibre, cabinets and network termination equipment serve your premises, so that they can check availability, install and repair the connection and attend appointments. Their engineers may need to enter your premises.

6.2 Mobile network operators and our mobile service partner, which carry and support our mobile services and bill us for your usage.

6.3 Other communications providers and industry bodies, including the switching hub operated by TOTSCo, your previous or new provider, the operators of the emergency services database and number portability processes, and directory providers, for the purposes described in clauses 4.7 and 5.2.

6.4 Service providers acting on our behalf, who process personal data under written contracts that require them to keep it secure and to use it only on our instructions. They include the providers of our billing, customer relationship and portal systems, payment and Direct Debit processing, email, text and telephony platforms, call recording, cloud hosting and data storage, engineering and installation contractors, security and reception services at our sites, printing and mailing, debt collection and IT support.

6.5 Credit reference agencies and fraud prevention agencies, as described in section 7.

6.6 Resellers, partners and wholesale customers. If your service is ordered through one of our partners, we share the information needed to provide and support it with that partner. If you are an end user of a provider that buys wholesale services from us, that provider is responsible for your personal data and its own privacy notice applies; we carry your traffic on its behalf and act on its instructions.

6.7 Professional advisers, insurers and auditors, including our lawyers, accountants and bankers, where they need the information to advise or act for us.

6.8 Regulators, public authorities and the courts, including Ofcom, the Information Commissioner (see section 15), the Communications Ombudsman, HM Revenue and Customs, the police and other law enforcement and public authorities and the courts, where the law requires or permits, or where it is necessary to establish, exercise or defend legal claims.

6.9 Prospective buyers, investors and successors, in the circumstances described in clause 4.15.

6.10 We do not sell personal data and we do not allow third parties to use it for their own marketing.

7. Credit reference and fraud prevention agencies

7.1 When you apply for services, and periodically while you are a customer, we may search your records at one or more credit reference agencies. They give us information about your credit history, the electoral register and the people you are financially linked with, which we use to assess whether we can provide services, on what terms and whether we need a

deposit. We tell you which agencies we use, and where to find their own privacy information (the Credit Reference Agency Information Notice), when we run a search or if you ask us.

7.2 The agencies keep a record of our search, which other lenders and providers may see, and we share information about your account with them, including how you manage payments and any default. If you apply jointly with another person, or tell us about a financial association, the agencies may link your records together. Information held by credit reference agencies is typically kept for six years.

7.3 The personal data you give us, and the information we collect about you, may be shared with fraud prevention agencies, who use it to prevent fraud and money laundering and to verify your identity. If fraud is detected, you could be refused certain services, finance or employment. Fraud prevention agencies can hold personal data for different periods, typically up to six years, and law enforcement agencies may access it. If you would like more information about how the fraud prevention agencies we use process your personal data, please contact us.

7.4 Some of these checks may result in a decision made automatically, for example to decline an order or to require a deposit. Section 13 explains the safeguards that apply and how you can ask for a person to review the decision.

8. Where your personal data is stored and international transfers

8.1 We are a UK company and we store and process personal data in the United Kingdom, including in our own data centres. Some of our service providers use systems, staff or support located outside the United Kingdom, and some Infrastructure Providers, mobile operators and roaming partners process data abroad when you use your service overseas.

8.2 Where personal data is transferred outside the United Kingdom we make sure it is protected by one of the safeguards permitted by data protection law: the destination is a country or organisation that the UK Government has decided provides adequate protection, which includes the European Economic Area; or we put in place the International Data Transfer Agreement or the UK Addendum to the European Commission's standard contractual clauses and satisfy ourselves, applying the data protection test required by law, that the standard of protection will not be materially lower than in the United Kingdom; or, occasionally, one of the specific exceptions in data protection law applies, such as where the transfer is necessary to perform your contract. You can ask us for details of the safeguards used for a particular transfer.

9. How long we keep your personal data

9.1 We keep personal data only for as long as we need it for the purposes described in this policy, to meet our legal, regulatory, tax and accounting obligations, and to establish, exercise or defend legal claims. When we no longer need it we delete it or anonymise it securely. Our main retention periods are as follows.

9.2 Account, contract, order and billing records: for as long as you are a customer and for six years after your account closes, which is the period within which a claim about the contract can be brought.

9.3 Enquiries and quotes that do not become an order: twelve months from your last contact with us.

9.4 Communications data (call records, connection and session records, IP address allocations): twelve months from creation, or longer where a retention notice under the

Investigatory Powers Act 2016 or a specific legal hold requires it.

9.5 Network security, performance and portal access logs: up to twelve months, unless they form part of an investigation.

9.6 Call recordings and web chat transcripts: twelve months, or for as long as needed to resolve a complaint, dispute or investigation to which they relate.

9.7 Complaints: six years from the date the complaint is closed.

9.8 Credit, identity and fraud check results: for the life of your account and six years after it closes; if we do not provide services to you, twelve months from the decision.

9.9 Additional support and vulnerability information: for as long as you are a customer, reviewed with you at least once a year, and removed when you ask us to or your account closes, unless we must keep it for a legal reason.

9.10 Marketing preferences: for as long as you are a customer or prospect. If you opt out we keep the minimum information needed to make sure we do not contact you again.

9.11 CCTV images: thirty days, unless an incident requires us to keep particular footage for longer.

9.12 Data centre and office visitor and access records: twenty-four months, or for the term of the relevant colocation contract and six years after it ends where the records evidence compliance with that contract.

9.13 Business, wholesale and partner contact records: for the life of the relationship and six years after it ends.

9.14 Website and portal analytics: for the periods set out in our Cookie Policy.

10. How we keep your personal data secure

10.1 We protect personal data using measures appropriate to the risk, including access controls and role-based permissions, encryption of data in transit and, where appropriate, at rest, network segregation, logging and monitoring, secure data centres with physical access control and CCTV, staff vetting and training, and regular testing of our systems and processes. As a communications provider we are also required to meet the security duties in the Telecommunications (Security) Act 2021, which include managing the security of our suppliers and reporting certain security incidents to Ofcom.

10.2 If a personal data breach occurs we will assess it and, where required, notify the Information Commissioner within 72 hours and tell you without undue delay if the breach is likely to adversely affect you or your privacy. We keep a record of all breaches, whether or not they are notifiable.

10.3 You can help by keeping your portal password and account security answers private, by using a strong and unique password, and by being alert to phishing. We will never ask you for your full password, and we will never ask you to pay by a method that is not shown on your bill or in the portal.

11. Our website, portal and social media

11.1 Our Cookie Policy explains the cookies and similar technologies we use on our website and portal and how you can manage them. We ask for your consent before using any cookies that are not exempt from the consent requirement. Data protection law now allows certain low-risk cookies, such as those used solely to collect statistical information to improve our website or to remember how you like the site to look, to be used without consent, provided we tell you about

them and give you a way to opt out; our Cookie Policy identifies any cookies of that kind and how to opt out.

11.2 Our availability checker uses the postcode and address you enter to check which services can be delivered there. We share that address with our Infrastructure Providers for that purpose and keep a record of the check so that we can follow up your enquiry and plan our network.

11.3 If you post a comment or review on our website we hold the details you enter and your IP address so that we can publish and moderate it and detect spam. Pages on our website may include content embedded from other sites, such as videos and maps, which behaves as if you had visited that site directly and may set that site's own cookies.

11.4 We run pages on Facebook, X and Instagram. When you interact with those pages we see the information you make available and may respond to you. The platforms process your personal data under their own privacy notices, and we receive only aggregated statistics from them about the use of our pages.

11.5 Our website contains links to other websites. This policy does not apply to those sites, and we are not responsible for how they use your personal data.

12. Your rights

You have the following rights under data protection law. Some of them apply only in certain circumstances, and we will explain if that is the case when you contact us.

12.1 Access. You can ask for a copy of the personal data we hold about you and information about how we use it. The law requires us to carry out a reasonable and proportionate search for the information you ask for.

12.2 Rectification. You can ask us to correct personal data that is inaccurate or to complete personal data that is incomplete.

12.3 Erasure. You can ask us to delete your personal data in certain circumstances, for example where we no longer need it. We cannot delete data we are required by law to keep, such as billing records and communications data subject to a retention notice.

12.4 Restriction. You can ask us to stop using your personal data, while continuing to store it, in certain circumstances, such as while we check its accuracy or consider an objection.

12.5 Portability. Where we process personal data you have given us by automated means on the basis of your consent or our contract, you can ask us to give it to you, or to send it to another provider, in a commonly used electronic format.

12.6 Objection. You can object to processing based on our legitimate interests. We will stop unless we can show compelling legitimate grounds that override your interests, rights and freedoms, or that the processing is needed for legal claims. You can object to direct marketing at any time and we will always stop.

12.7 Withdrawing consent. Where we rely on your consent you can withdraw it at any time. This does not affect processing carried out before you withdrew it, and we may still be able to process the same data on another lawful basis, which we will explain to you.

12.8 Automated decisions. Where a decision that has a significant effect on you is made solely by automated means you have the rights described in section 13.

12.9 Complaints. You can complain to us and to the Information Commissioner, as described in section 15.

12.10 To exercise any of these rights, contact us using the details in section 2. We may need to check your identity, or that you are authorised to act for the person concerned, before we act. We will respond within one month of receiving your request, or of receiving the identity or clarification information we need. If a request is complex, or you have made several, we may extend that period by up to two further months and will tell you if so. We do not charge for dealing with requests unless a request is manifestly unfounded or excessive, in which case we may charge a reasonable fee or decline to act.

12.11 To stop marketing you can use the unsubscribe link in any email, reply STOP to any marketing text, change your preferences in the portal, or contact us. You may also register with the Telephone Preference Service and the Mailing Preference Service, which we screen against; registering will not stop service messages about your account.

13. Automated decision-making and profiling

13.1 We use automated systems to support the credit, identity and fraud checks described in section 7, to detect and block security threats on our network, and to tailor the offers and information we show you. Most of the outcomes are reviewed by a person before they affect you.

13.2 Where a decision that has a legal or similarly significant effect on you, such as declining an order or requiring a deposit, is made solely by automated means, we will tell you that this has happened, explain the decision as far as the law allows, and give you the opportunity to make representations, to obtain human intervention and to contest the decision. We do not make solely automated decisions of this kind using special categories of personal data.

13.3 If an automated security measure, such as the blocking of traffic that appears malicious, affects your service and you believe it is mistaken, please contact us and a member of our network team will review it.

14. Children

14.1 Our services are provided to adults aged 18 or over and our website and portal are not directed at children. We do not knowingly collect personal data from anyone under 18 except where an account holder tells us about a member of their household for the purposes of support or safeguarding. If you believe a child has given us personal data, please contact us and we will remove it.

14.2 The account holder is responsible for the use of the services at their premises, including by children. Parental control tools are available on request to help you manage the content that can be accessed over your connection.

15. Complaints

15.1 If you think we have not handled your personal data in accordance with data protection law, you have the right to complain to us. You can do so through the contact form on our website, by email, by telephone or by post using the details in section 2, or in any other way that reaches us. We will acknowledge your complaint within 30 days of receiving it, look into it without undue delay, keep you informed of its progress and tell you the outcome. We keep a record of every data protection complaint and how it was resolved.

15.2 You can also complain, at any time, to the Information Commissioner, the independent regulator for data protection in the United Kingdom, at Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF, by telephone on 0303 123 1113, or online at ico.org.uk. The Information Commissioner's Office is being reconstituted as the Information Commission under the Data (Use and Access) Act 2025, and references in

this policy to the Information Commissioner include the Information Commission once that change takes effect. We would welcome the chance to resolve your concern first, so please contact us before you approach the regulator if you can.

15.3 Complaints about the service itself, rather than about your personal data, are handled under our Complaints Code of Practice, which is published on our website and explains how to escalate to the Communications Ombudsman.

16. Changes to this policy

16.1 We review this policy at least once a year and whenever our services or the law change. The version number and

effective date are shown at the top of this policy, and the current version is always published on our website. If we make a change that materially affects you we will tell you, for example by email, by a message in the portal or on your bill, before it takes effect.

16.2 Version history. Version 1.0, 17 August 2020: original website privacy policy. Version 2.0, 1 September 2026: complete rewrite to reflect the Data (Use and Access) Act 2025 reforms to UK data protection and e-privacy law, our obligations as a communications and data centre provider, and the full range of services we now offer.